UNIVERSITY OF MALAYA

INFORMATION COMMUNICATIONS TECHNOLOGY

In order to use the Information Communications Technology **["ICT"]** facilities of the University of Malaya **["UM"]** you MUST have affirmed this electronic form.

By clicking the "**I Agree**" button below, I acknowledge that **I have read and understood** the **"Dasar Keselamatan ICT UM"** and **"ICT Rules And Regulations For The Use Of Computing Facilities"** and "**Siswamail Terms and Condition**"of UM.

I **Further Acknowledge that I have** regularly referred to the UM Website: UM ICT-POLICY, RULES & GUIDELINES for any changes to the Rules and Regulations.

ICT Declaration

I AM AWARE that the very act of using UM computer facilities or connecting any equipment including computer, notebook, server, mobile devices, wireless devices and electronic gadgets to the UM network through whatsoever means (wired or wireless), construes that **I AGREE** to abide by all relevant UM Rules and Regulations. It is my responsibility to ensure that I keep up-to-date with these Rules and Regulations. **I AM FURTHER AWARE** that the Rules and Regulations are available on the UM ICT Services section of the UM website.

I AM AWARE that my use of the UM computer room machines and any equipment I attach to the UM network may be monitored for legal purposes and for my and UM's security.

I AGREE that in the event of an investigation into my computer and/or network use, a copy may be taken of the contents of my computer's hard disk and stored securely pending the outcome of the investigation. Such a copy will only be stored and used for the duration of an investigation after which it will be destroyed.

I AM AWARE that, after giving reasonable notice, the stored copy will be available for my inspection.

I AGREE that I am expected to access my UM e-mail regularly and I understand that my UM e-mail account will be the primary means of contacting me by any authorised UM employee. As certain communications may be time critical, I **FURTHER AGREE** to check and respond, if necessary, to those e-mails within THREE (3) working days.

I AM AWARE that I MUST have Anti-Virus protection appropriate for my computer's operating system and that it automatically updates my computer from a trusted source.

I AM AWARE that I MUST download and install all security patches and updates for my computer operating system from a trusted source.

UM ICT RULES AND REGULATIONS FOR THE USE OF COMPUTING FACILITIES

Access to Facilities

1. If you connect any device (wired or wireless) to the University network, you MUST abide by all terms contained in the University ICT Rules and Regulations and any policies and guidelines governing them. See: **http://ptm.um.edu.my/?modul=Guidelines&pilihan=ICT_Rules_And_Guidelines**

2. Access to the University **network may be suspended or terminated if you are** i**n** violation of any of these Rules and Regulations. Not withstanding this, you may also be subject to disciplinary action under the University's student disciplinary rules. Reinstatement of computer facilities is subject to an appeal to the CIO.

3. In order to use the University's Information Systems and access the wireless network you must create a UM's official Email account through an online Form and affirm your ICT Declaration. To use computer room facilities, please refer to your respective Faculty for details.

Use of Facilities

4. By using the University computer room facilities or connecting any equipment to the University network you agree to abide by all University ICT Rules and Regulations. It is your responsibility to stay up-to-date with these Rules and Regulations.

5. Your computer MUST have up-to-date anti-virus software that updates automatically from a trusted software vendor. You will be disconnected from the network if your computer becomes infected with viruses, malware or if it displays suspicious network activity.

6. Your computer MUST be kept up-to-date with operating system updates and security patches. Failure to install system and security patches may leave your computer vulnerable to viruses, malware and malicious attacks which could result in your computer being disconnected from the network.

7. You are solely responsible for the actions of ANY person who accesses your own personal computer by whatsoever means.

8. The use of any file-sharing software or participation in Peer-to-Peer (P2P) file-sharing networks is prohibited unless prior written permission is obtained from the CIO. The file-sharing networks may include, but is not limited to, Kazaa; Napster; Gnutella; Morpheus; iMesh; Grokster; Limewire; NEOnet; Oxtella; Edonkey; eMule; Undernet; Bit Torrent; Aimster; WinMX; and Azureus. If you are found to have P2P software running on your computer you will be subject to appropriate action by the University.

9. You MUST comply with all the internal laws of the University and the national laws governing the use of computing facilities, whether directly or indirectly.

10. Unless otherwise prior written permission is obtained from the CIO, you are prohibited from running any network service on any computer in your possession which may include IIS; Apache; SMB/CIFS; Samba; DNS; DHCP; WINS; Internet Connection Sharing (wired or wireless); File and Printer sharing. Running unauthorised services can lead to security vulnerabilities and can cause connection problems for you and other network users.

11. ONLY laptop and desktop computers are allowed on the University network. You MUST NOT connect any wireless access point, cable/broadband router, hub, switch, femtocell, game console or any such devices to the UM network without written permission from the CIO.

12. You should not knowingly create, transmit, receive or handle any material on UM ICT equipment that may be offensive to any employee and student of the University or the public. Any attempt to access UM facilities or another user's computer, account or e-mail; or impersonate as another user or create or introduce programs with malicious intent; or involve in software theft; or use UM facilities to harass any company or individual; or send chain or junk mail, may result in appropriate action by the University.

13. You MUST keep your passwords secure. Do not disclose them to, or allow them to be used by any other person. You should notify the CIO immediately if you suspect that your University password has been compromised.

14. The UM network and the computer room facilities are for use for academic work only and should not be used for any personal or commercial purposes.

15. You MUST NOT attempt to access or alter restricted portions of the operating system in the computer (e.g. registry) or configuration (e.g. IP Address, Computer Name and Active Directory settings) in the computer room facilities unless authorized by the appropriate University's representative (Wakil ICT). You are required to take reasonable care of these facilities and report faults immediately to the respective representative.

16. No food or drink shall be taken into or consumed in the computer rooms. Repairs to computers damaged by food crumbs or drink spills will be charged at full cost to the individuals responsible.

17. No smoking is allowed in the computer rooms or its vicinity.

18. Any attempt to circumvent network and computer security restrictions imposed by the University (for example running an encrypted tunnel or changing your computer's MAC address) may be subject to appropriate action by the University.

19. You MUST NOT prepare, upload, download, save, store or use any material containing pornographic elements, unlicensed software and other applications such as electronic games, video and music which will interfere with the normal operation of computers, terminals, peripherals, or networks.

Monitoring and securing the network

20. The PTM logs all network traffic in order to detect problems and to ensure the network is operating correctly. The logs record usernames, MAC addresses, IP addresses of clients and servers, traffic type, application classification and amount of data transferred.

21. In the event of a network fault, or a case of serious network abuse (from within the University or from outside), it may be necessary to actively record certain network traffic. This is done only to record particulars under investigation, and will be restricted to just the activities of a computer or any service. Any recorded data will be discarded as soon as possible.

22. Any investigation into network use will be done with the express permission of CTO. User under investigation shall have the right to a fair hearing and given an opportunity to submit any written representation.

23. The University occasionally runs network scans to detect any unauthorised devices or services or any security vulnerabilities to protect the University network and its users. If any unauthorised devices or services is detected, the University will contact the owner of the computer. You are required to ensure that your computer's name has been set to be your UM Matriculation Number to enable the Universityto identify you and render any assistance.

24. The University has installed firewalls to prevent unauthorised access to the network and services. You may contact PTM should there be any interference in your use of the University network.

PUSAT TEKNOLOGI MAKLUMAT (PTM), AUGUST 2011

The above rules and regulations are also available online in the **IT Policy and Regulations** section of The PTM, UM website – http://ptm.um.edu.my -> Guideline -> ICT Rules & Guidelines

SISWAMAIL : TERMS AND CONDITIONS

SISWAMAIL is an official email application system provided to all student of University of Malaya.

Your use of SiswaMaiL web site application and services (referred to collectively as the "Services" in this document) is subject to the terms and conditions between you and SiswaMaiL.

In order to use the Services, you must agree to the Terms and Conditions. As a SiswaMaiL users, you are considered to accept all the terms and conditions below:

1. **Use of the Services**

In order to access certain Services, you may be required to provide information about yourself (such as Identification and Matriculation Number, or Contact details) as part of the registration process for the Service, or as part of your continued use of the Services. You agree that any registration information you give to SiswaMaiL will always be accurate, correct and up-to-date.

You AGREE that you will not engage in any activity that interferes with or disrupts the Services (or the servers and networks which are connected to the Services).

2. **Your password and account security**

You will receive a password and account designation upon completing the Service's registration process. You are responsible for maintaining the confidentiality of the password and account and are fully responsible for all activities that occur under your password or account.

You AGREE to :

- immediately notify Siswa Admin of any unauthorized use of your password or account or any other breach of security, and
- ensure that you exit from your account at the end of each session.

You AGREE and UNDERSTAND that you are responsible for maintaining the confidentiality of passwords associated with any account you use to access the Services.

3. **Prohibited Actions**

You AGREE not to use the Service to:

- upload, post, email, transmit or otherwise make available any Content that is unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable;
- upload, post, email, transmit or otherwise make available any unsolicited or unauthorized advertising, promotional materials, "junk mail," "spam," "chain letters," "pyramid schemes," or any other form of solicitation, except in those areas (such as shopping) that are designated for such purpose;
- upload, post, email, transmit or otherwise make available any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;
- Create multiple user accounts in connection with any violation of the Agreement or create user accounts by automated means or under false or fraudulent pretenses
- Conduct or forward pyramid schemes and the like
- Impersonate another person (via the use of an email address or otherwise) or otherwise misrepresent yourself or the source of any email
- Illegally transmit another's intellectual property or other proprietary information without such owner's or licensor's permission
- Promote or encourage illegal activity
- Transmit content that may be harmful to minors
- Use SiswaMaiL to violate the legal rights (such as rights of privacy and publicity) of others

4. **Account Inactivity**

Your SiswaMaiL account is valid throughout your studies.
Your account will be terminated immediately after you have finished your studies in University of Malaya.

5. **Changes To The Terms**

Siswa Admin reserves the right to revise its policies at any time.

6. **Miscellaneous**

Siswa Admin shall not be held responsible for any loss however caused resulting from any suspension or unavailability of any service.

You are responsible for any material stored on your SiswaMaiL accounts. We shall not be held responsible for any loss, however caused, of this material.

UM reserves the right to give your email address to 3rd party for the University's programme purposes.

Refer : Google Apps Terms

- Legal Notices
- Privacy Policy
- Program Policies
- Terms of Service

PUSAT TEKNOLOGI MAKLUMAT (PTM), AUGUST 2011